Claims

1. A method of verifying that a host coupled to an IP network is authorised to use an IP address which the host claims to own, the IP address comprising a routing prefix and an interface identifier part, the method comprising receiving from the host one or more components, applying a one-way coding function to the or each component and/or derivatives of the or each component, and comparing the result or a derivative of the result against the interface identifier part of the IP address, wherein if the result or its derivative matches the interface identifier the host is assumed to be authorised to use the IP address and if the result or its derivative does not match the interface identifier the host is assumed not to be authorised to use the IP address.

2. A method according to claim 1, wherein said components comprise a hash value being one of a sequence of related hash values.

3. A method according to claim 1, wherein said components comprise a public key or a digest of a public key generated by said host or obtained by said host from another authorised party or a fixed bit sequence of the same length.

4. A method according to claim 1, wherein said components comprise an initial interface identifier which corresponds to or is derived from a link layer address of the host, or a fixed bit sequence of the same length.

5. A method according to claim 1, wherein said components comprise an initial interface identifier which corresponds to or is derived from a link layer address of the host, or a zero bit sequence of the same length.

6. A method according to claim 2, wherein said components comprise a counter value which identifies the position of the received hash value in said sequence.

7. A method according to claim 2, wherein said series of hash values are derived at the host by applying a one-way coding function to a seed value and a public key or a digest of the public key.

8. A method according to claim 2, wherein said series of hash values are derived at the host by applying a one-way coding function to a seed and an initial interface identifier.

9. A method according to claim 2, wherein said series of hash values are derived at the host by applying a one-way coding function to a seed, a public key or a digest of the public key, and an initial interface identifier.

10. A method according to claim 2, and comprising deriving a hash value from the received hash value to provide a derivative to which the one-way coding function is applied, the derived hash value being the last hash value in the sequence.

11. A method according to claim 10, wherein in the event of a first IP address verification, the hash value received from the host is the hash value preceding the final hash value in the sequence and for each subsequent verification process, the next previous hash value must be received.

12. A method of generating an IP address at a host, the IP address comprising a routing prefix and an interface identifier part, the method comprising generating the interface identifier part by applying a one-way coding function to one or more components, wherein said components include a hash value which is generated using a random number.

13. A method according to claim 12, wherein the said hash value is generated by applying a one-way coding function to a combination of the random number and an initial interface identifier.

14. A method according to claim 12, wherein the said hash value is generated by applying a one-way coding function to a combination of the random number and a public key or a digest of the public key.

15. A method according to claim 12, wherein the said hash value is generated by applying a one-way coding function to a combination of the random number, an initial interface identifier, and a public key or a digest of the public key.

16. A method of avoiding the duplication of IP addresses in an IP network when a new host attaches to the network, the method comprising the steps of:

generating an Interface Identifier at the new host by combining a component or components and/or derivatives of the component or components using a one-way coding function, and using the result of the coding function or a derivative of said result as the interface identifier, the interface identifier forming part of said IP address;

sending a neighbour solicitation message from the new host to other hosts already attached to the access network;

receiving a neighbour advertisement message at the new host from each other host claiming to own said IP address, the or each neighbour advertisement message containing said component(s); and

for each received neighbour advertisement message

combining the component(s) and/or derivatives of the component(s) using said coding function; and

comparing the result or a derivative of the result against the interface identifier part of the IP address, wherein if the result or the derivative matches the interface identifier the host from which the neighbour advertisement message is received is assumed to be authorised to use the IP address and if the result or its derivative does not match the interface identifier that host is assumed not to be authorised to use the IP address.

17. A method of verifying that a host coupled to an IP network is authorised to use an IP address which the host claims to own, and that the host is able to receive data packets sent to that address, the method comprising:

carrying out the method of the above first aspect of the invention to confirm that said host is authorised to use the IP address;

sending a challenge to the host using said IP address as the destination address for the challenge;

receiving a response from the host; and

verifying that the received response is a correct response to the challenge.

18. A method according to claim 17, wherein said challenge is a randomly generated number and the response comprises the challenge.

19. A method according to claim 17, wherein said challenge comprises said IP address concatenated with a randomly generated number, and the response comprises the IP address concatenated with the challenge.

20. A method according to claim 17, wherein said challenge is formed by applying a one-way coding function to said IP address concatenated with a randomly generated number, and the response is formed by applying a one-way coding function to the IP address concatenated with the challenge.

21. A method of authenticating a public key transmitted over an IP network from a first to a second host, the method comprising:

at said first host, generating an interface identifier using said public key and combining the interface identifier with a routing prefix to form an IP address for the first host;

sending said public key from the first to the second node over said IP network; and

at said second node, verifying that said public key was the key used to generate said interface identifier.

22. A method of binding an IP address to a host, the IP address comprising a routing prefix and an interface identifier part, the method comprising:

generating said interface identifier by combining one or more components and/or derivatives of the components using a coding function; and

generating a certificate, signed with a private key of a public-private key pair belonging to the host, the certificate containing the interface identifier and ones of said components or said derivatives or further derivatives, such that the certificate can be authenticated using the host's public key, and ownership of the interface identifier can

be verified by reconstructing the interface identifier using the contents of the certificate, and comparing the result against the true interface identifier.